REMARKS/ARGUMENTS

Favorable consideration of this application, as presently amended, is respectfully requested.

Claims 1-10, 12, 14, 15 and 17-25 are pending in the present application. Claims 1-10, 13, 14, 15 and 17-25 are amended by the present response. Support for additions and amendments to the claims is found in the disclosure as originally filed, at least on page 13, lines 17-24. Thus, no new matter is added.

In the outstanding Action, the specification was objected to as including informalities; Claims 2-6, 8-10, 14 and 17-25 were objected to as including informalities; Claims 1-25 were rejected under 35 U.S.C. §112, second paragraph as indefinite; Claims 1-10, 12, 14, 15 and 17-25 were rejected under 35 U.S.C. §103(a) as unpatentable over Newcombe (U.S. Pat. Pub. No. 2003/0172269) in view of Arnold et al. (WO 03/055170, herein "Arnold").

With regard to the objection to the specification as including informalities, the specification has been amended to overcome the objection. Thus, Applicants respectfully request that the objection to the specification be withdrawn.

With regard to the objection to Claims 2-6, 8-10, 14 and 17-25 as including informalities, these claims have been amended to overcome the objection. Thus, Applicants respectfully request that the objection to Claims 2-6, 8-10, 14 and 17-25 be withdrawn.

With regard to the rejection of Claims 1-25 under 35 U.S.C. §112, second paragraph as indefinite, Applicants respectfully submit that Claims 1-3, 6-8, 10, 12, 14, 15, 17, and 19-25 have been amended to overcome the rejection.

Accordingly, Applicants respectfully request that the rejection of Claims 1-25 under 35 U.S.C. §112, second paragraph be withdrawn.

Addressing now the rejection of Claims 1-10, 12, 14, 15 and 17-25 under 35 U.S.C. §103(a) as unpatentable over Newcombe and Arnold, Applicants respectfully traverse this rejection.

Claim 1 recites,

> In an authentication system in which an authentication server which authenticates a user, a user terminal which transmits a user authentication information, and an application server which provides a service to the user through the user terminal are connected together to enable a communication therebetween through a network, the address based authentication system including:
>
> the authentication server which comprises
>
> authentication means for authenticating a user based on the user authentication information transmitted as an authentication request from the user terminal;
>
> an address allocating means for allocating an address to the user terminal for a successful authentication of the user;
>
> generating means for generating information-for-authentication using at least the allocated address;
>
> a ticket issuing means for issuing a ticket containing the allocated address information-for-authentication;
>
> and a ticket transmitting means for transmitting the ticket issued by the ticket issuing means to the user terminal;
>
> the user terminal which comprises
>
> transmitting means for transmitting the user authentication information to the authentication server for purpose of an authentication request;
>
> a ticket reception means for receiving the ticket containing the allocated address transmitted from the authentication server;
>
> means for setting up the allocated address contained in the ticket as a source address for each packet which is to be transmitted from the user terminal to the application server;
>
> means for transmitting a first packet including the ticket to the application server for establishing a session; and
>
> a service request means for transmitting a second packet requesting the service to the application server through the session;
>
> and the application server which comprises
>
> a ticket memory means for storing the ticket transmitted from the user terminal;
>
> ticket verifying means for verifying the presence or absence of any forgery in the information-for-authentication in the ticket transmitted from the user terminal and storing the ticket in the ticket memory means in the absence of a forgery;

> an address comparison means for determining whether or not the allocated address contained in the ticket which is stored in the ticket memory means coincides with the source address of the second packet which is transmitted from the user terminal through the session; and
>
> a service providing means for transmitting to the user terminal packets which provide the service to the user when a coincidence between the addresses is determined by the address comparison means.

Newcombe describes an application authentication system (AAS) that authenticates a client in response to the client's request, and sends a content ticket containing local and remote IP addresses to the client. Further, in the system of Newcombe, the client sends the content ticket to a content server as a content request. In response, the content server checks if the IP address in the received content ticket matches the source address of the received packet which contains the content ticket. If they match, the content server transmits the content to the client.

Arnold describes a system that includes a server which authenticates a user and allocates the user an IP address. Further, in Arnold a session is established between the server and a user computer. In addition, the server always monitors the user's access to the network through the session so that authentication can be achieved between the user and a service provider through the session.[1]

Applicants note that Arnold teaches at page 12, lines 1-9 that a server instance 110 allocates an IP address to a user; however, the server instance 110 is intended to set a VPN (virtual private network) between the server instance 110 and the user computer, and is not relevant to either the claimed authentication server or the authentication server 402 in Newcombe. The server instance 110 operates like a gateway and is directly involved in controlling communication traffic of the user terminal such that the user terminal establishes communication with a desired e-shop through the VPN, i.e., through the server instance 110.

[1] See page 4, second and third paragraphs of Arnold.

In contrast, the claimed authentication server involves the authentication of a client and issuance of tickets. Thus, the allocation of an address by the authentication server in the claimed invention is unique and is not taught in either Newcombe or Arnold.

Furthermore, Newcombe discloses in paragraph [0048] that a local and remote IP addresses of a client are included in a content ticket; however, these addresses are not ones that have been allocated by the authentication server but are ones that have been received from the client as part of a request for a content ticket (as is explained in lines 7-11 of paragraph [0025] and lines 3-6 of paragraph [0052]), or ones that are extracted from a TCP/IP header associated with the client's request as is explained on the 6th to 4th lines from the end of paragraph [0025].

In Newcombe's paragraph [0072], it is described that "the server readable portion may include information associated with the client's local and remote IP addresses....and a session key." In addition, it is described that "the server readable portion is encrypted with a public encryption key associated with the receiving content server." However, the local and remote IP addresses are not ones that have been allocated by the authentication server 402.

In Newcombe's paragraph [0052], it is described that "clients are enabled to provide information associated with local and remote IP addresses to AAS (application authentication system) 108 as part of the request for content tickets." In other words, the authentication server 108 inserts the local and remote IP addresses received from the client into the server readable portion. This insertion of IP addresses is not equivalent to checking the authenticity of the IP addresses.

As was pointed out in the outstanding Action with respect to storing of the ticket, it is described in paragraph [0056] that the authentication data store 408 stores tickets. However, these tickets are not ones that are received by the content server from the users.

Paragraph [0125] certainly describes that "at block 1302, the client is authenticated by the content server," and it is checked whether the time of the ticket is expired (step 1402), whether the ticket is revoked (step 1404), or whether the ticket includes an access grant (step 1406). However, since the ticket does not contain information-for-authentication generated by the authentication server using at least ***an address allocated by the authentication server***, Newcombe never describes checking authenticity of the claimed information-for-authentication.

Regarding the address comparison, the outstanding Action states that the comparison of the local and remote IP addresses "may be one check for authenticity but not the most important one." Further the outstanding Action states that "if a client is behind a NAT, the remote IP address presented by the client and locally discovered IP address will be different" and, therefore, "a missmatch does not definitely make the client unauthentic."

Initially, Applicants note that the address comparison performed at the decision block 712 described in paragraph [0098] of Newcombe belongs to one of the procedures performed when client tries to interact with authentication server to obtain a TGT (ticket granting ticket) in block 502 of Fig. 5, which is detailed in Fig. 6, particularly, by block 602 which is further detailed in Fig. 7 including the block 712. In other words, the address comparison is performed at the block 712 by the authentication server but not by the content server. Moreover, the address comparison acts merely to determine whether the client is behind NAT or not (i.e., if the local address differs from the remote address, the client is decided to be behind NAT) and ***does not determine authenticity***.

It is natural that when a client device is behind a NAT, the client device has a locally allocated IP address which has to be different from a remote address (a global address) allocated when accessing the Internet. However, the claimed invention is not concerned with the case where the client device (i.e., user terminal) is behind a NAT. The address allocated

by the authentication server is used as a source address of each packet when making access to the application server on the network. Such address cannot be a local address to be used behind NAT.

Furthermore, the outstanding Action states that "real authentication come from decrypting the server readable portion of the ticket to obtain the address stored inside and comparing that the client's local source address [0091]". However, in [0091] of Newcombe, there is no description of comparing client's local address and remote address. It should be noted that the server readable portion is encrypted by the authentication server 402 using a public encryption key associated with the ticket granting server 404 (4th to 2nd lines from the end of paragraph [0091]) so that only the ticket granting server 404 can read the encrypted portion. Assuming that the public encryption key is accessible by everyone, everyone can produce an encrypted server readable portion and, therefore, everyone can generate a ticket including such an encrypted portion. Therefore, in Newcombe, there is no assurance that the server readable portion in the ticket is actually produced by the authentication server 402.

Even though the address in the server readable portion is compared with the address extracted from a TCP/IP header, the comparison is nothing more than a comparison between two pieces of information both provided by the same client. In such a case, a node (such as a rogue access point) maliciously installed on the network between a client and a content server could easily masquerade as an IP address of the client. That is, in Newcombe's system, it is not possible to determine with certainty the actually identity of the IP address. This drawback results from the fact that the ticket does not contain an address allocated by an authentication server based on user authentication.

On the other hand, in the claimed invention, the ticket issued by the authentication server contains information-for-authentication which is generated by the authentication server using at least the allocated address which is allocated by the authentication server. Since the

allocated address has been allocated to a user terminal by the authentication server and contained in the ticket together with the information-for-authentication generated by the application server, it is ensured that the allocated address in the ticket received by the application server has surely been issued by the authentication server and, by comparing the allocated address in the ticket to the source address of the received packet, it is possible to guarantee that the user terminal which has sent the packet containing the ticket is exactly the same as the user terminal whose user has been authenticated by the authentication server.

In order to clarify the features of the Newcombe's system, Applicants would like to summarize the entire procedure in the Newcombe's system as follows:

a) A client sends a request for a content ticket to an application authentication system (AAS) 108, the request including information associated with client's local and remote IP addresses. See paragraph [0052].

b) Authentication server 402 in AAS 108 extracts the client's remote IP address from a TCP/IP packet and compares it to the remote IP address within the request to determine if the client is valid or not. See paragraph [0061].

c) If the authentication server 402 determines that the user (client) is valid, the authentication server 402 provides the client with a ticket granting ticket (TGT) which includes a server readable portion, client readable portion and time stamp. See paragraph [0062].

d) A ticket granting server (TGS) 404 in the AAS 108 validates the server readable portion of the TGT received from the user (client) and provides the valid user (client) with a content ticket that enables access to the content server. See paragraphs [0068], lines 1-4 and [0071], lines 1-4.

The content ticket may include a server readable portion encrypted with a public encryption key associated with the content server. The server readable portion may include client's local and remote IP addresses. See paragraph [0072], lines 7-14.

e) Then, the client sends the content ticket to the content server which authenticates the client at block 1302 by examining the address and modified authenticator as detailed in Fig. 11, and also authenticates the ticket at block 1306 by examining the ticket information as detailed in Fig. 14. See paragraphs [0124] and [0125].

f) If the ticket is authentic, the content server sends the requested content to the client. See paragraph [0127], lines 8-10.

Thus, it is apparent that the address authenticated by the content server is nothing other than the address the client has originally provided regardless of whether the address is valid one allocated to the authenticated user or not.

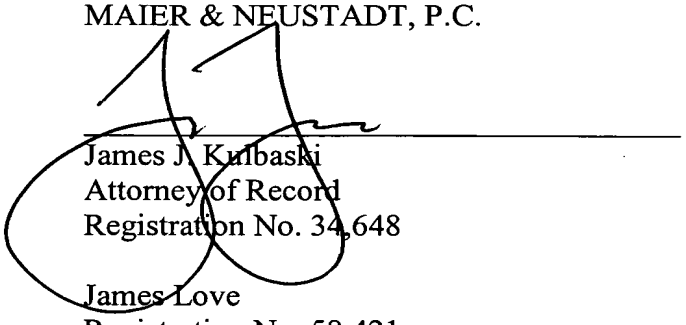
Accordingly, Applicants respectfully submit that Claim 1 patentably distinguishes over Newcombe and Arnold considered individually or in combination.

Furthermore, Applicants respectfully submit that Claims 7, 12, 14, 15 and 21-23 also patentably distinguish over Newcombe and Arnold for similar reasons.

Consequently, in view of the present amendment, no further issues are believed to be outstanding in the present application, and the present application is believed to be in condition for formal allowance. A Notice of Allowance for the claims is earnestly solicited.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbaski
Attorney of Record
Registration No. 34,648

James Love
Registration No. 58,421

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

1698236_1